

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-117173

(43) 公開日 平成10年(1998) 5月6日

(51) Int.Cl. ⁶	識別記号	F I	
H 0 4 H	1/00	H 0 4 H	1/00 F
H 0 4 K	1/00	H 0 4 K	1/00 Z
H 0 4 N	7/16	H 0 4 N	7/16 C
	7/167		7/167 Z

審査請求 未請求 請求項の数11 O L (全 10 頁)

(21) 出願番号	特願平8-269938	(71) 出願人	000004226 日本電信電話株式会社 東京都新宿区西新宿三丁目19番2号
(22) 出願日	平成8年(1996)10月11日	(72) 発明者	早川 和宏 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72) 発明者	福永 博信 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72) 発明者	渡部 智樹 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(74) 代理人	弁理士 若林 忠

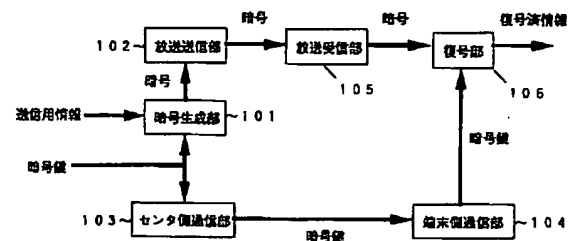
最終頁に続く

(54) 【発明の名称】 情報配信装置および情報受信装置

(57) 【要約】

【課題】 暗号化された情報を多数の利用者に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険を小さくする。

【解決手段】 暗号生成部101は送信用情報と暗号鍵を受け取り、送信用情報を暗号化して出力する。放送送信部102は暗号を受け取り不特定多数に対して放送する。センタ側通信部103は暗号鍵を受け取り、通信路を通じて送信する。端末側通信部104は通信路を通じて暗号鍵を受け取り、出力する。放送受信部105は放送された暗号を受信し出力する。復号部106は暗号と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が入力されない場合は動作を行わない。



【特許請求の範囲】

【請求項1】 情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する情報配信装置。

【請求項2】 情報を暗号化して配信する情報配信装置であって、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された前記情報を含む情報を放送する放送送信手段と、前記暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する情報配信装置。

【請求項3】 請求項1の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項4】 前記暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する請求項3記載の情報受信装置。

【請求項5】 請求項2の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項6】 前記照合情報は前記暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて前記情報配信装置との通信路の接続／切断を行なう通信路制御手段を有する、請求項5記載の情報受信装置。

【請求項7】 請求項2の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報に関する関連情報と前記照合情報を得て両者を照合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された情報を復号する復号手段とを有する情報受信装置。

【請求項8】 請求項2の情報配信装置で暗号化された情報を受信する情報受信装置であって、暗号化された情報を含む情報を受信する放送受信手段と、前記暗号鍵を含む前記照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された前記情報を含む情報から暗号化された前記情報に関する関連情報を分離する関連情報分離手段と、前記関連情報と前記照合情報を得て両者を照

合し、復号が許可された場合のみ前記照合情報を出力する照合情報出力手段と、前記照合情報から前記暗号鍵を分離する暗号鍵分離手段と、暗号化された前記情報と前記暗号鍵を得て暗号化された前記情報を復号する復号手段とを有する情報受信装置。

【請求項9】 前記関連情報は、暗号化された情報の情報識別子を含み、前記照合情報は、復号できる情報の情報識別子の一つ以上を含み、前記照合情報出力手段は前記照合情報に含まれる情報識別子の中に、前記関連情報に含まれる情報識別子が含まれていることを、前記照合情報を出力する条件とする請求項8記載の情報受信装置。

【請求項10】 前記関連情報は、暗号化された情報の秘匿度を表す数値を含み、前記照合情報は、復号できる情報の秘匿度を表す数値を含み、前記照合情報出力手段は前記関連情報に含まれる秘匿度が、前記照合情報に含まれる秘匿度以下であることを、前記照合情報を出力する条件とする請求項8記載の情報受信装置。

【請求項11】 前記関連情報は、暗号の復号方法を指示する情報を含み、前記照合情報出力手段は前記関連情報に含まれる暗号の復号方法に従い前記照合情報受信手段を制御して照合情報を取得する請求項8記載の情報受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報を暗号化して不特定多数に対して放送し、受信者のみが受信した暗号化された情報を復号する情報配信・受信システムに関する。

【0002】

【従来の技術】放送において受信者を限定したい場合、放送内容を暗号化して暗号鍵を持つものだけが暗号を復号して放送内容を知ることができるようにするのが一般的である。たとえば、有料放送では放送内容を暗号化し、受信料を支払う受信者のみが暗号を復号することができるようにする必要がある。これを実現するため、従来は復号装置に付加するハードウェアを用意しこれに暗号鍵を記録したものか、あるいは復号装置の一部もしくは全体を、暗号を復号する権利のある者に提供する方法が採られていた。

【0003】また、有料放送のように「見た分だけ課金する」ことが必要の場合は、復号操作を行ったことに対する課金処理、または復号を行った際の料金徴収者への通知を自動的に行えることが望ましい。このため、暗号を復号する装置においては、暗号が復号される条件を情報提供者の側で制御することができるか、あるいは暗号が復号されたことを確実に情報提供者に伝えることができる装置が要求される。従来、この目的のためには復号操作を行ったことをICカードなどのハードウェアに記録し、この記録を情報提供者が定期的に回収することで課金等を行っていた。

【0004】

【発明が解決しようとする課題】これらの方法は、復号装置や暗号鍵の複製により、復号する権利のない者が復号を行う可能性や、ICカードに記録されたデータを改変され、正常に課金が行えない可能性があった。また、ICカードその他の付加的なハードウェアに対するコスト、復号操作を行った記録を回収するコスト等がかかり、有料情報提供サービスのコストアップの原因となっていた。

【0005】本発明の目的は、暗号化された情報を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい情報配信装置および情報受信装置を提供することにある。

【0006】

【課題を解決するための手段】本発明の第1の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を通信路を通じて送信する暗号鍵送信手段とを有する。また、本発明の第1の情報受信装置は、放送された情報を含む情報を受信する放送受信手段と、暗号鍵を通信路を通じて受信する暗号鍵受信手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0007】このシステムでは利用者は暗号と暗号鍵を常に受信しているので、送信側では任意の時刻に暗号鍵を変更することができる。したがって、多数の利用者へ暗号を放送することにより情報配信を行う際に、暗号鍵の複製や不正使用が行われる危険を小さくすることができる。

【0008】本発明の実施態様によれば、暗号鍵受信手段は、新しい暗号鍵が得られるまで古い暗号鍵を保持する。

【0009】回線断後も暗号鍵を保持することができるので、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、この装置が有用である。

【0010】本発明の第2の情報配信装置は、情報と暗号鍵を得て前記情報を暗号化する暗号生成手段と、暗号化された情報を含む情報を放送する放送送信手段と、暗号鍵を含む照合情報を通信路を通じて送信する照合情報送信手段とを有する。本発明の第2の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0011】本発明の実施態様によれば、情報受信装置は、照合情報が暗号鍵の有効期間の情報を含み、該有効期間の情報に基づいて情報配信装置との通信路の接続／

切断を行なう通信路制御手段を有する。これによりシステムの運用上の利便性が高まる。

【0012】本発明の第3の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報に関する関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0013】あらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。

【0014】本発明の第4の情報受信装置は、暗号化された情報を含む情報を受信する放送受信手段と、暗号鍵を含む照合情報を通信路を通じて受信する照合情報受信手段と、暗号化された情報を含む情報から暗号化されている情報に関する関連情報を分離する関連情報分離手段と、関連情報と照合情報を得て両者を照合し、復号が許可された場合のみ照合情報を出力する照合情報出力手段と、照合情報から暗号鍵を分離する暗号鍵分離手段と、暗号化された情報と暗号鍵を得て暗号化された情報を復号する復号手段とを有する。

【0015】本発明の実施態様によれば、関連情報は、暗号化されている情報の情報識別子を含み、照合情報は、復号できる情報の情報識別子の一つ以上を含み、照合情報出力手段は照合情報に含まれる情報識別子の中に、関連情報に含まれる情報識別子が含まれていることを、照合情報を出力する条件とする。

【0016】本発明の実施態様によれば、関連情報は、暗号化されている情報の秘匿度を表す数値を含み、照合情報は、復号できる情報の秘匿度を表す数値を含み、照合情報出力手段は関連情報に含まれる秘匿度が、照合情報に含まれる秘匿度以下であることを、照合情報を出力する条件とする。

【0017】暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。

【0018】本発明の実施態様によれば、関連情報は、暗号の復号方法を指示する情報を含み、照合情報出力手段は関連情報に含まれる暗号の復号方法に従い照合情報受信手段を制御して照合情報を取得する。

【0019】照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。

【0020】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0021】図1は本発明の第1の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0022】暗号生成手段である暗号生成部101は送信用情報と暗号鍵を受け取り、送信用情報を暗号化して出力する。放送送信手段である放送送信部102は暗号化された情報を受け取り、不特定多数に対して放送する。暗号鍵送信手段を含むセンタ側通信部103は暗号鍵を受け取り、通信路を通じて送信する。暗号鍵受信手段を含む端末側通信部104は通信路を通じて暗号鍵を受け取り、出力する。放送受信手段である放送受信部105は放送された暗号化された情報を受信し、出力する。復号手段である復号部106は暗号化された情報と暗号鍵を受け取り、復号済み情報を出力するが、暗号鍵が10入力されない場合は動作を行わない。ここで、暗号生成部101と放送送信部102とセンタ側通信部103は情報配信装置を構成し、放送受信部105と端末側通信部104と復号部106は情報受信装置を構成している。

【0023】したがって、図1のシステムでは通信を行って暗号鍵を受信しての間だけ復号部106が動作する。

【0024】このシステムでは、その時点で送信される暗号と対応しているかぎりにおいて、暗号鍵を任意の時間に変化させてよい。したがって、受信側では情報を復号する必要がある間、常に通信路を通じて暗号鍵を受け取り続ける必要がある。

【0025】なお、通信路としては、端末側からセンタ側へ情報を送る必要はないので、一般的な双方向通信サービスのほか、同報通信サービスを利用することができる。

【0026】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる通信サービスを利用する場合には、受信者が暗号鍵を受信したことを確認できる。したがって、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。

【0027】図2は本発明の第2の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0028】暗号生成手段である情報サーバ201は送信したい情報を受け取って暗号化し、放送送信手段である送信装置202を通じて放送用衛星に向けて送信する。また同時に、暗号鍵を暗号鍵送信手段であるモデム203を通じて専用線による通信路へ送出する。放送受信手段である受信装置205は衛星からの電波を受信し、暗号化された情報を出力する。同時に、暗号鍵受信手段であるモデム204は通信路から暗号鍵を受信し、出力する。復号手段である復号部206は暗号化された情報を暗号鍵を用いて解読し、復号済み情報を出力する。ここで、情報サーバ201と送信装置202とモデム203は情報配信装置を構成し、モデム204と受信装置205と復号部206は情報受信装置を構成している。

【0029】情報サーバ201は任意の時間に暗号鍵を変更する。したがって、暗号を持続的に復号することができるのは通信路に接続されている情報受信装置のみとなる。

【0030】以上の説明では通信路として専用線を想定したが、通常の電話回線やCATV回線も使用可能である。

【0031】なお、端末側通信部105、モデム204は、回線断後も暗号鍵を保持するようにしてもよい。この場合、通信回線を切断しても次に暗号鍵が変化するまでは復号を続けることができる。通信回線として電話回線を使用する場合は、通信料金削減の点から、有用である。

【0032】図3は本発明の第3の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0033】暗号生成部301、放送送信部302、放送受信部305、復号部308の機能はそれぞれ図1中の暗号生成部101、放送送信部102、放送受信部105、復号部106の機能と同様である。

【0034】照合情報生成部303は暗号鍵を受け取り、暗号鍵に任意の情報を付加した照合情報を生成し、出力する。照合情報送信手段であるセンタ側通信部304は照合情報を受け取り、通信路を通じて送信する。照合情報受信手段である端末側通信部306は通信路を通じて照合情報を受け取り、出力する。暗号鍵分離手段である暗号鍵抽出部307は照合情報を受け取り、暗号鍵を抽出して出力する。ここで暗号生成部301、放送送信部302、照合情報生成部303、センタ側通信部304は情報配信装置を構成し、放送受信部305、端末側通信部306、暗号鍵抽出部307、復号部308は情報受信装置を構成している。

【0035】本システムでは、暗号鍵に関する付加情報を照合情報に含めて通信する。付加情報としては暗号鍵が作成された時刻、暗号鍵の有効期間、復号アルゴリズム識別子、放送サービスのサービス識別子、サービス提供者識別子などを用いることができる。端末側通信部306が照合情報を保持できる場合は、照合情報の中に例えば暗号鍵の有効期間を含めておき、受信側の通信路制御手段でこれを参照して暗号鍵の有効期間が切れるまでは通信回線を切断しておくことができる。

【0036】図4は本発明の第4の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0037】暗号生成部401、放送送信部402、照合情報生成部403、センタ側通信部404、端末側通信部406、暗号鍵抽出部408、放送受信部405、復号部409の機能はそれぞれ図3中の暗号生成部301、放送送信部302、照合情報生成部303、センタ側通信部304、端末側通信部306、暗号鍵抽出部307、放送受信部305、復号部308の機能と同様である。

【0038】照合情報出力手段である照合部407は関連情報と照合情報を受け取り、照合情報と関連情報を比較して復号が許可される場合のみ照合情報を出力する。

【0039】ここで、暗号生成部401、放送送信部402、照合情報生成部403、センタ側通信部404は情報配信装置を構成し、放送受信部405、端末側通信部406、照合部407、暗号鍵抽出部408、復号部409は情報受信装置を構成している。

【0040】照合情報と関連情報は暗号化されている情報の復号を許可するか否かにかかわる情報を用いることができる。たとえば照合情報で送られたパスワードと関連情報で入力されたパスワードが一致した場合のみ復号を許可するという使い方が可能である。この場合は、一般に行われているように、照合情報で送信するパスワードは逆変換が不可能な演算をあらかじめ施してから送信し、関連情報に対して同じ演算を行った結果と比較すれば、照合情報の中からパスワードを盗まれる危険はない。

【0041】図1から図3のシステムでは通信回線に接続できれば必ず暗号を復号することができるが、図4のシステムではあらかじめ正しい関連情報を受信者が入手している場合に限り復号を行うことができるので、情報の受信者をより限定することができる。

【0042】図5は本発明の第5の実施形態の情報配信・受信システムの構成を示すブロック図である。

【0043】暗号生成部501、照合情報生成部503、センタ側通信部504、端末側通信部505、暗号鍵抽出部509、復号部510の機能は図4中のそれぞれ暗号生成部401、照合情報生成部403、センタ側通信部404、端末側通信部406、暗号鍵抽出部408、復号部409の機能と同様である。

【0044】放送送信手段である放送送信部502は暗号化された情報と関連情報を受け取り、両者を含む放送信号を生成し、不特定多数に対して放送する。放送受信手段である放送受信部506は放送信号を受信し出力する。関連情報分離手段である関連情報分離部507は放送信号を受け取り、暗号と関連情報を抽出して出力する。照合情報出力手段である照合部508は関連情報と照合情報を比較し、比較結果により復号が許可される場合のみ照合情報を出力する。

【0045】ここで、暗号生成部501、放送送信部502、照合情報生成部503、センタ側通信部504は情報配信装置を構成し、端末側通信部505、放送通信部506、関連情報分離部507、照合部508、暗号抽出部509、復号部510は情報受信装置を構成している。

【0046】関連情報は暗号化されている情報に関する情報である。たとえば暗号に含まれている情報を表す情報識別子、情報の秘匿度を表す数値などである。一方、照合情報は暗号鍵の他に、関連情報と対応する復号許可

情報を含む。復号許可情報は暗号鍵が用いられる条件を記述した情報である。例としては、一つまたは複数の情報を表す情報識別子や復号できる情報の秘匿度を表す数値などである。

【0047】照合情報生成部503を複数用いてそれぞれ異なる情報識別子や情報秘匿度を含む照合情報を生成し、異なる通信チャネルを用いて送信すれば、受信側が復号できる情報を、どの通信チャネルに接続するかにより決定することができる。

10 【0048】図6は本発明の第6の実施形態の情報配信・受信システムの構成を示すブロック図である。このシステムはCS放送においてスクランブル暗号化されたMPEG2パケットの暗号鍵を通信路を通じて取得する。ここでは通信路として電話回線を想定する。また、このシステムでは放送番組と共にその番組の種類に関する情報が放送される。一方、通信路では暗号鍵のほかにその暗号鍵を使用できる番組の種類を送信する。受信側では、この番組の種類に従って、暗号を復号するか否かを決定する。

20 【0049】タイマ601は一定時間毎に暗号鍵更新要求を出力する。暗号鍵生成部602は暗号鍵更新要求を受けると新しい暗号鍵を生成し出力する。照合情報生成部605は暗号鍵に許可する番組の種類を付加して出力する。図7は照合情報に用いる番組の種類に関する情報の一例を示す図である。生成された照合情報はモデム606を通じて通信路へ送信される。照合情報は、一つのセンタから複数の利用者へ送信する必要があるため、同報型の通信サービスを利用する。暗号生成手段である暗号生成部603は暗号鍵とMPEG符号を受け取り暗号を生成して出力する。放送送信手段であるCS放送装置604は関連情報と暗号を受け取り、放送パケットとして衛星を通じて放送する。関連情報には図7と同じ形式で現在放送中の番組のジャンルを示す情報が含まれる。放送受信手段であるCS受信装置608は衛星からの放送を受信し放送パケットを出力する。関連情報分離手段である関連情報分離部611は放送パケットを受け取り、関連情報と暗号を分離し、出力する。受信側モデム607は照合情報を通信路から受信し出力する。照合情報出力手段である照合部609は照合情報と関連情報を受け取り、関連情報中の番組ジャンルが照合情報中の番組ジャンルに含まれていれば照合情報を出力する。暗号鍵分離手段である暗号鍵抽出部610は照合情報から暗号鍵を抽出し出力する。復号手段である復号部612は暗号と暗号鍵を受け取り、暗号を復号して得られるMPEG符号を出力する。

30
40
50 【0050】ここで、タイマ601、鍵生成部602、暗号生成部603、CS放送装置604、照合情報生成部605、モデム606は情報配信装置を構成し、モデム607、CS受信装置608、照合部609、暗号鍵抽出部610、関連情報分離部611、復号部612は

情報受信装置を構成している。

【0051】以上の説明では関連情報と照合情報には番組のジャンルに関する情報を持たせたが、ジャンル以外の情報を持たせることもできる。図8は関連情報に番組識別子、照合情報に複数の番組識別子のリストを持たせ、リストに示された番組のみ復号可とする例である。また、図9は関連情報には番組のレベル、照合情報にはその照合情報で復号を許可する番組のレベルを持たせ、そのレベル以下の番組のみ復号可とする例である。

【0052】また、図6において関連情報の中に照合情報10を入手する際に必要な同報型通信サービスの電話番号を含めておけば、モデム607をこの電話番号に対して発呼するように制御することにより、照合情報の入手先が目的に応じて複数存在しても、自動的に照合情報を取得することができる。

【0053】

【発明の効果】以上説明したように、本発明は、下記のような効果がある。

(1) 請求項1と3の発明は、暗号の復号に必要な暗号鍵を頻繁に変更することができるので、暗号化された情報20を多数の利用者に同時に配信する際に、不正な利用者が復号を行ったり、暗号鍵を複製する危険が小さい。

【0054】また、通信路として、電話網のように受信者が受信していることを交換機等の通信網上の装置で確認し記録することができる場合には、受信者が暗号鍵を受信したことを確認できるので、情報に対して課金する際に、通信履歴に基づいて課金額を決定することができる。これは有料放送をスクランブラ/デスクランブラを用いて行う際に、見た分だけ課金することを可能にする。

(2) 請求項4の発明は、請求項1と3からなるシステムの機能を短い通信時間で実現することができる。

(3) 請求項2と5と6の発明は、暗号鍵の有効期間など付加的な情報を通信することにより、装置の運用上の利便性を高めることができる。

(4) 請求項2と7の発明は、復号を行う際に、復号を行う者が正しい利用者かどうかを受信者の側で試験することができる。

(5) 請求項8、9、10の発明は、暗号が暗号鍵に対応するものであるかどうかを復号を行わずに試験することができる。この機能は、ある特定の情報を、特定の受信者集合に対して、復号を許可するかどうかを送信側で指定するために用いることができる。たとえば有料放送で、ある一定の課金額の通信チャンネルを通じて暗号鍵を取得している利用者が、どの番組を視聴することができるかを指定することができる。

(6) 請求項11の発明は、照合情報の請求先が複数存在する場合でも、暗号に対応した適切な照合情報を取得することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図2】本発明の第2の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図3】本発明の第3の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図4】本発明の第4の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図5】本発明の第5の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図6】本発明の第6の実施形態の情報配信・受信システムの構成を示すブロック図である。

【図7】本発明の第5、第6の実施形態において照合情報に含まれる情報の例を示す図である。

【図8】本発明の第5、第6の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

【図9】本発明の第5、第6の実施形態において照合情報に含まれる情報および照合部の動作の一例を示す図である。

【符号の説明】

101	暗号生成部
102	放送送信部
103	センタ側通信部
104	端末側通信部
105	放送受信部
106	復号部
201	情報サーバ
202	送信装置
30	203 モデム
204	モデム
205	受信装置
206	復号装置
301	暗号生成部
302	放送送信部
303	照合情報生成部
304	センタ側通信部
305	放送受信部
306	端末側通信部
40	307 暗号鍵抽出部
308	復号部
401	暗号生成部
402	放送送信部
403	照合情報生成部
404	センタ側通信部
405	放送受信部
406	端末側通信部
407	照合部
408	暗号鍵抽出部
50	409 復号部

501 暗号生成部

502 放送送信部

503 照合情報生成部

504 センタ側通信部

505 端末側通信部

506 放送受信部

507 関連情報分離部

508 照合部

509 暗号鍵抽出部

510 復号部

601 タイマ

602 暗号鍵生成部

603 暗号生成部

604 CS放送装置

605 照合情報生成部

606 モデム

607 モデム

608 CS受信装置

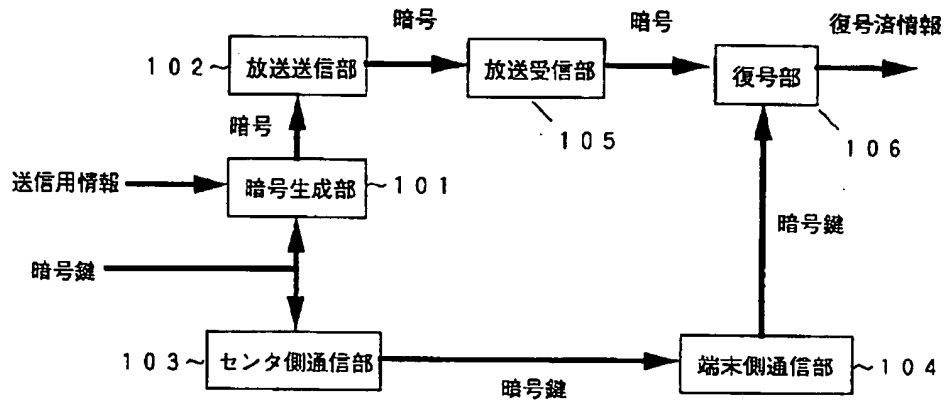
609 照合部

610 暗号鍵抽出部

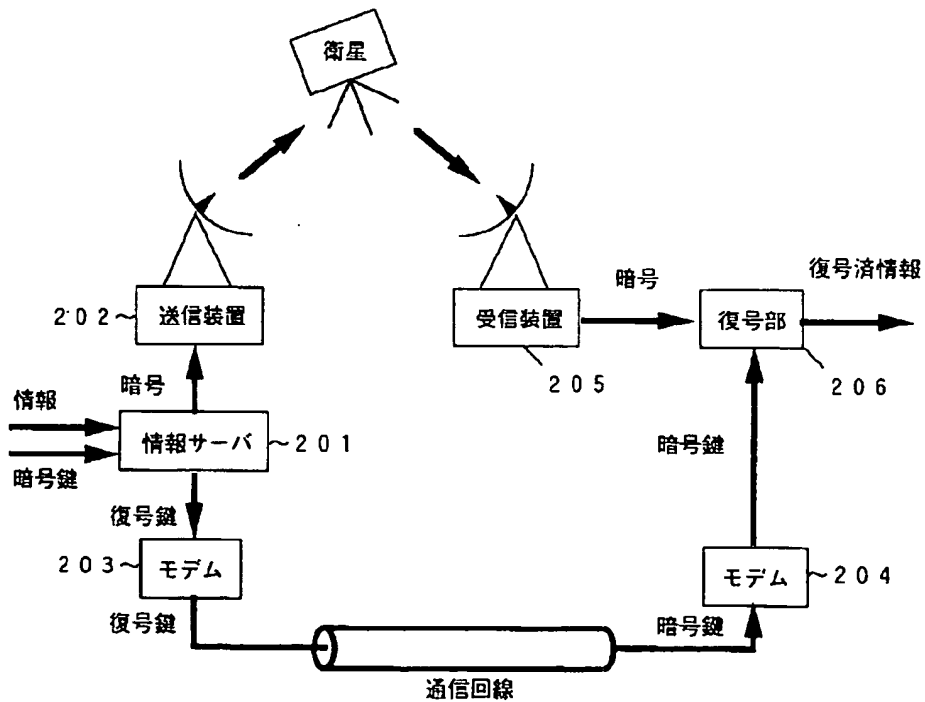
10 611 関連情報分離部

612 復号部

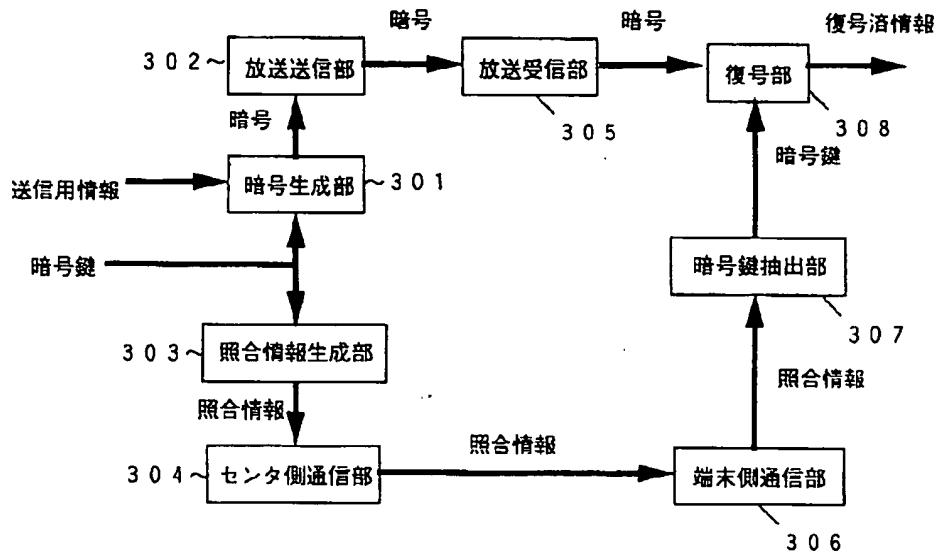
【図1】



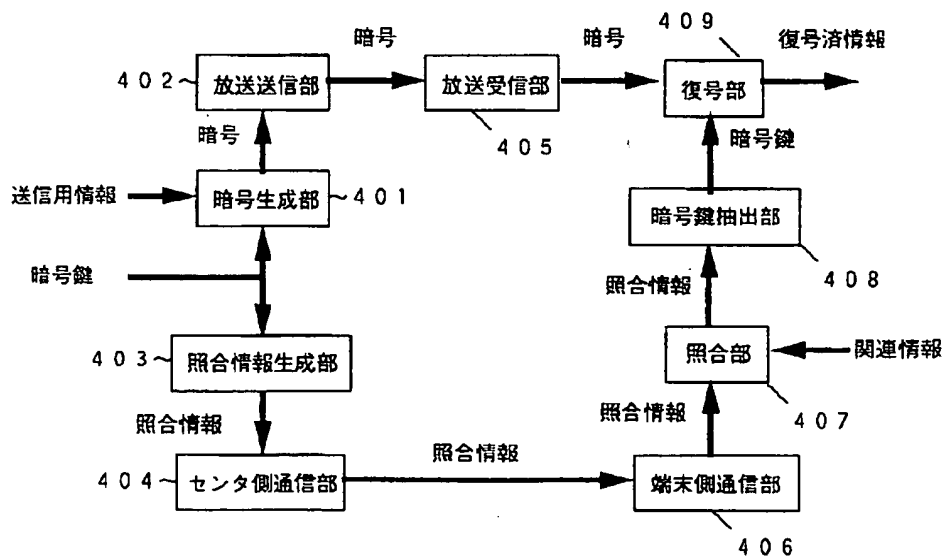
【図2】



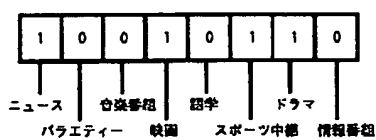
【図3】



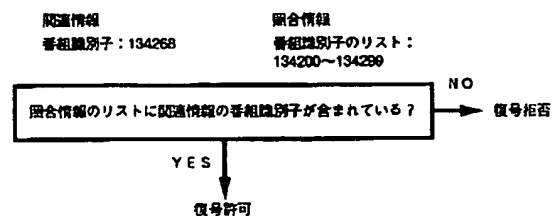
【図4】



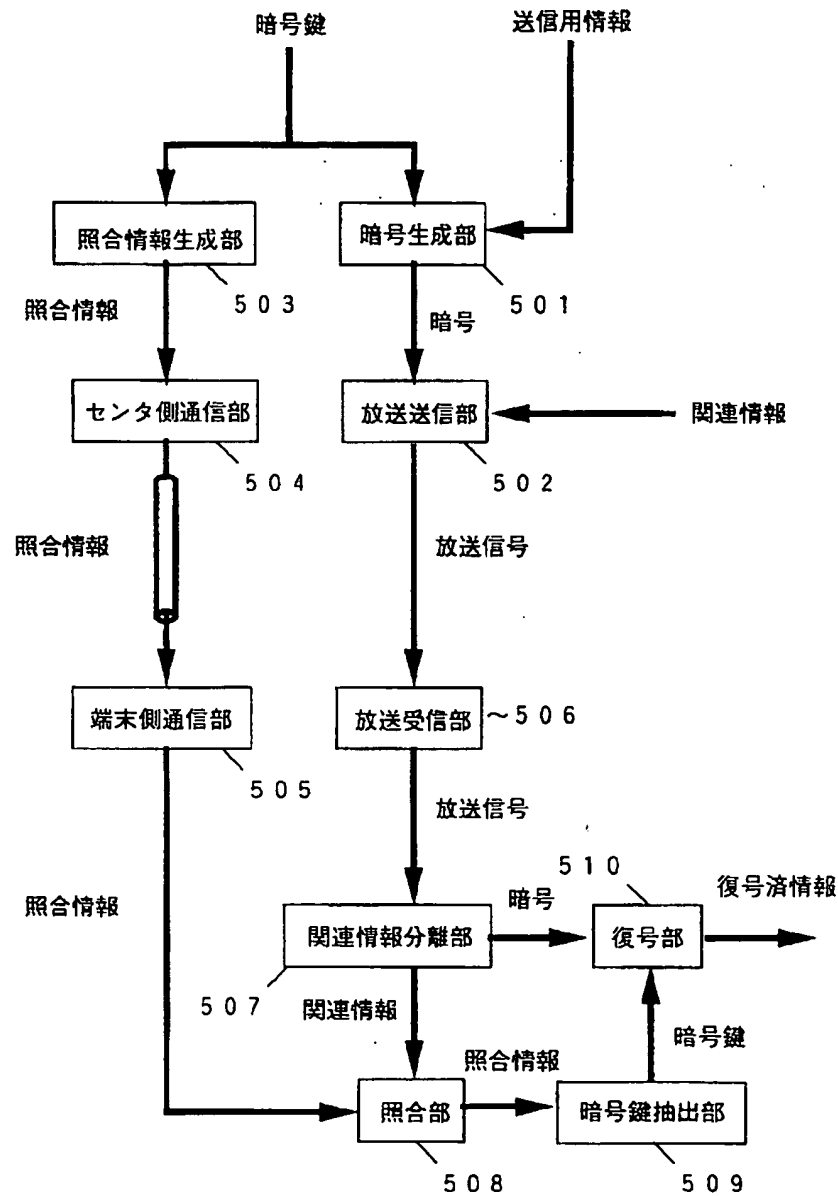
【図7】



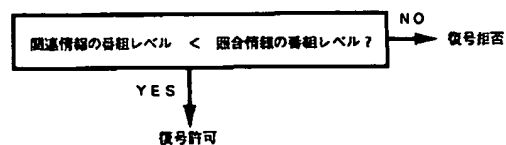
【図8】



【図5】



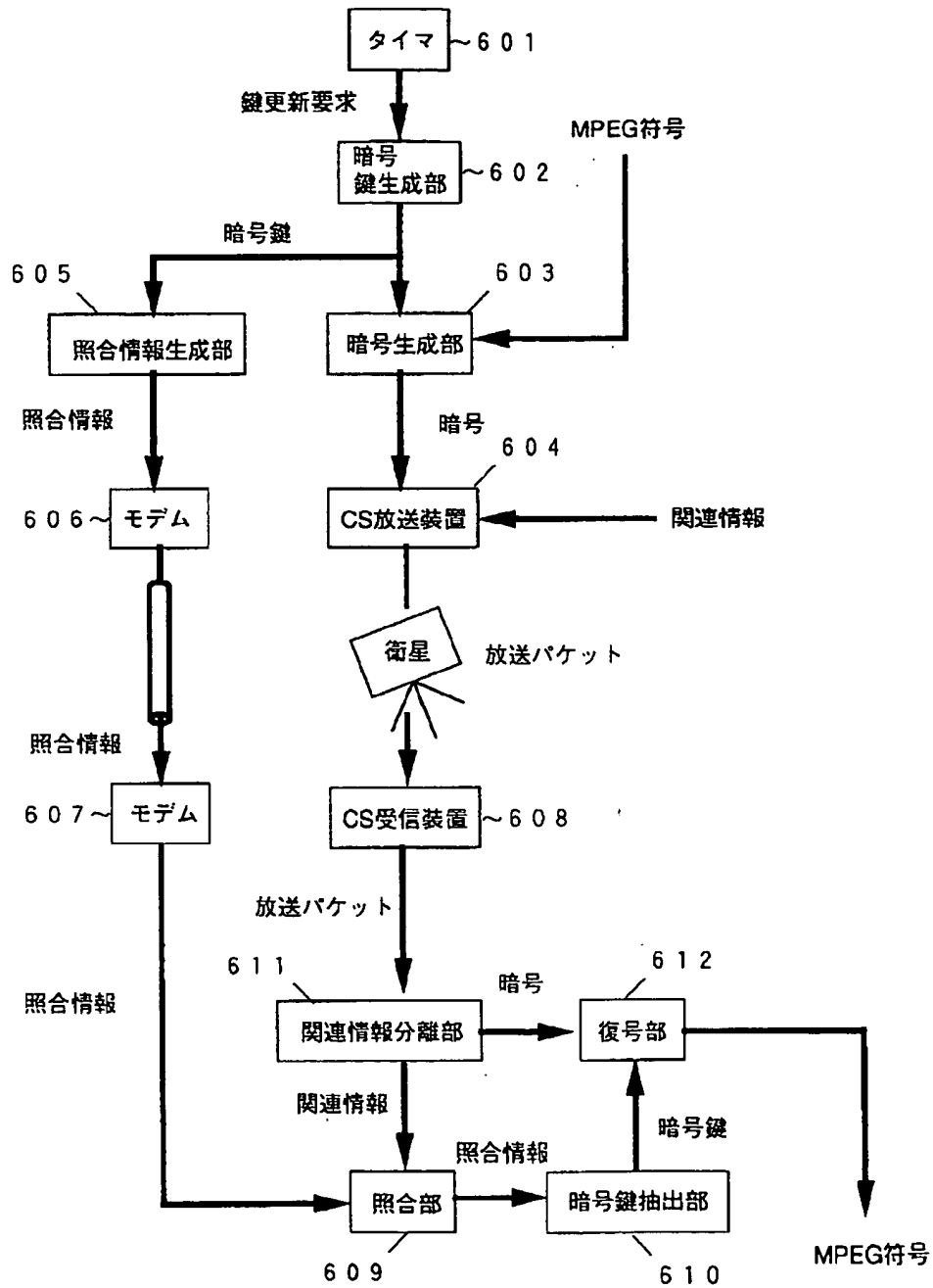
【図9】



番組レベルの例

- レベル1: 映画、スポーツ中継、バラエティを除く全番組
- レベル2: 映画、スポーツ中継を除く全番組
- レベル3: スポーツ中継を除く全番組
- レベル4: 全番組

【図6】



フロントページの続き

(72)発明者 鈴木 達郎
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 熊谷 佳子
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内